NSTB
National SCADA Test Bed
enhancing control systems security in the energy sector

Cyber Effects Analysis
Using
Virtual Control System Environment (VCSE)

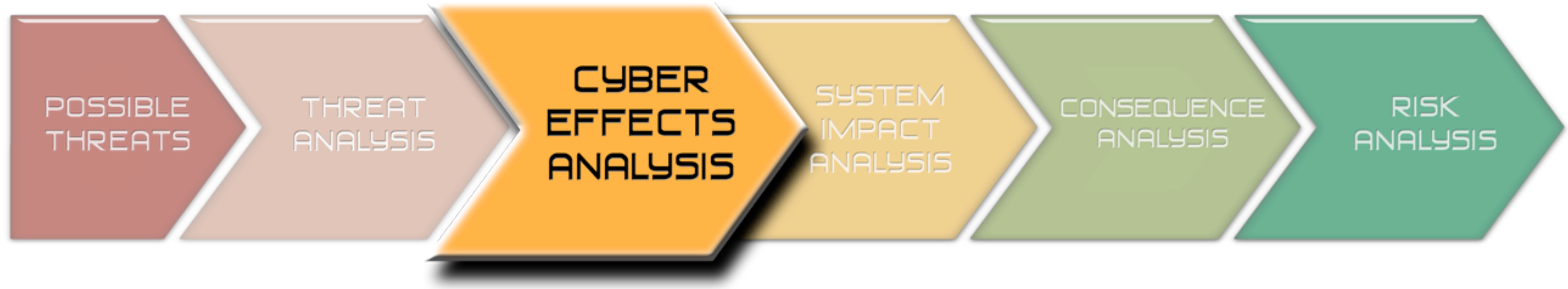
Greg Conrad
Sandia National Laboratories

U.S. Department of Energy
Office of Electricity Delivery
and Energy Reliability

Sandia National Laboratories

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

Threat-to-Consequence Framework



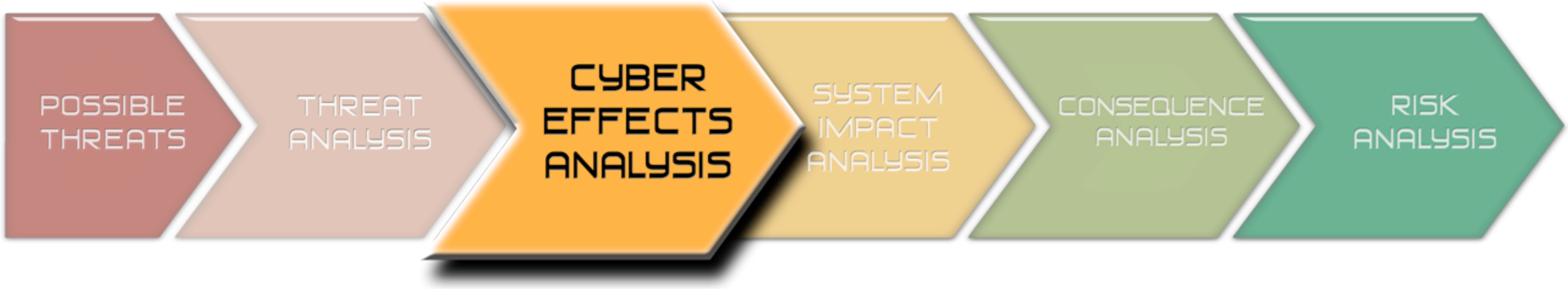
Challenges/Needs

- Develop a Control Systems Simulation Environment
- Model existing and future control system devices and communication protocols
- Design a scalable architecture to allow for Hardware-in-the-Loop

Results/Benefits

- Increase security awareness
- Understand impacts
- Reduce testing costs

Threat-to-Consequence Framework



- **How feasible is the Rogue Software Scenario?**
- **Where did the attack originate?**
- **How did the attack affect service?**
- **How capable is the adversary carrying out this attack?**
- **How does the severity of the attack change the effects?**
- **What other factors can change the scenario outcome?**
- **Can this happen to me?**

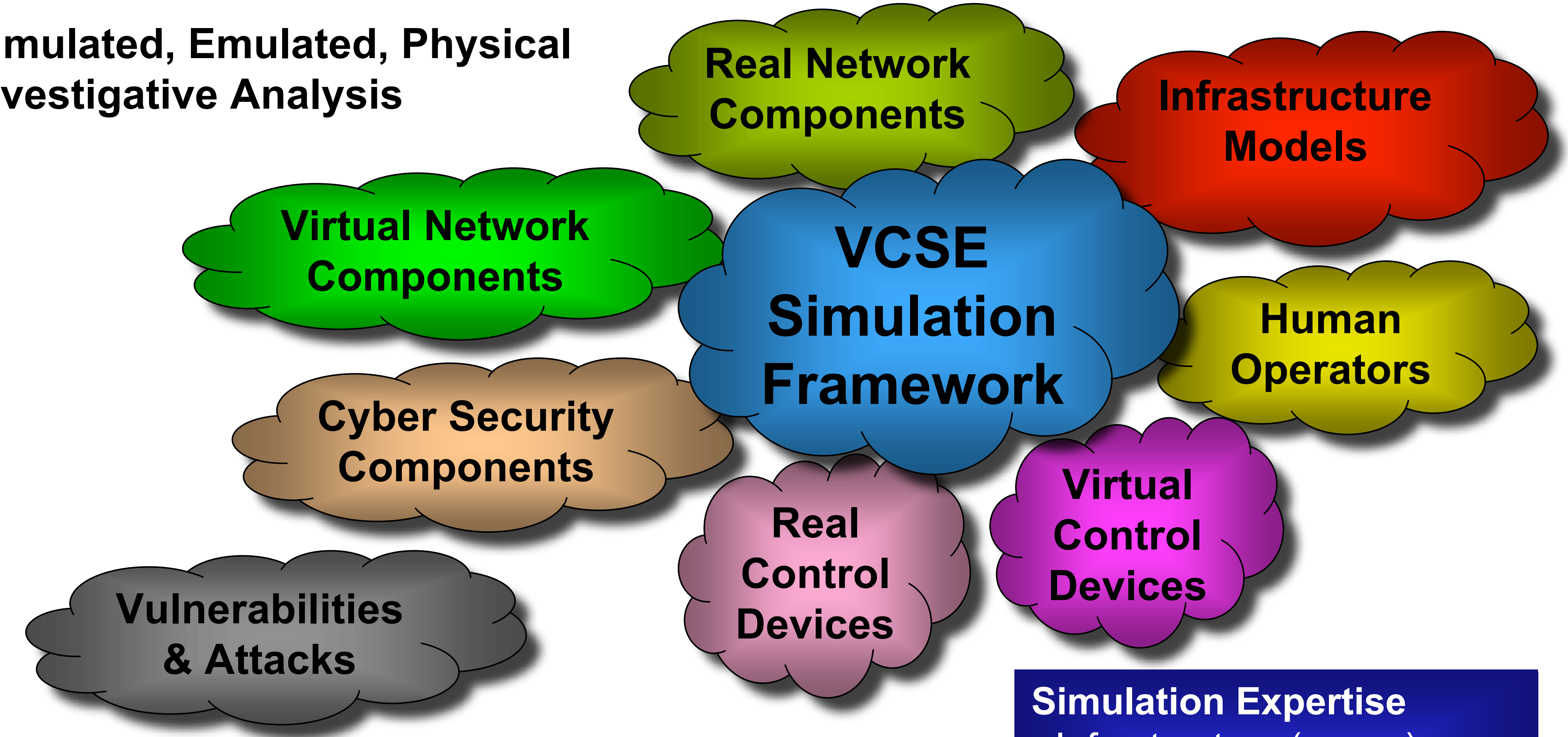
Virtual Control Systems Environment (VCSE) can be used to answer these questions

Overview

- Describe the Cyber Effects Analysis tools (VCSE)
- Describe how we analyzed the Rogue Software Attack with the tools
- Demonstrate the simulation
- Discuss the results
- Discussion

VCSE – A Hybrid Mod/Sim Test Bed

Simulated, Emulated, Physical Investigative Analysis



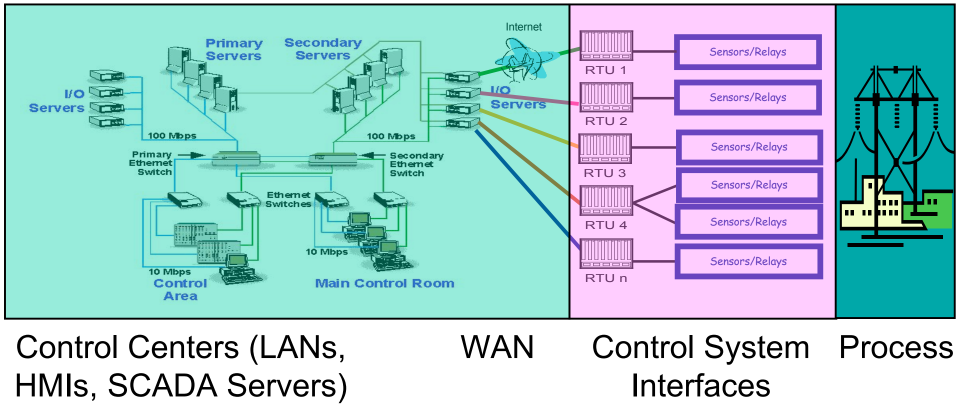
Analysis requirements dictate the extent that a VCSE component is utilized

Simulation Expertise
- Infrastructure (power)
- Control System
- Networking
- Cyber Security/Vulnerability
- Modeling & Simulation

What VCSE Provides

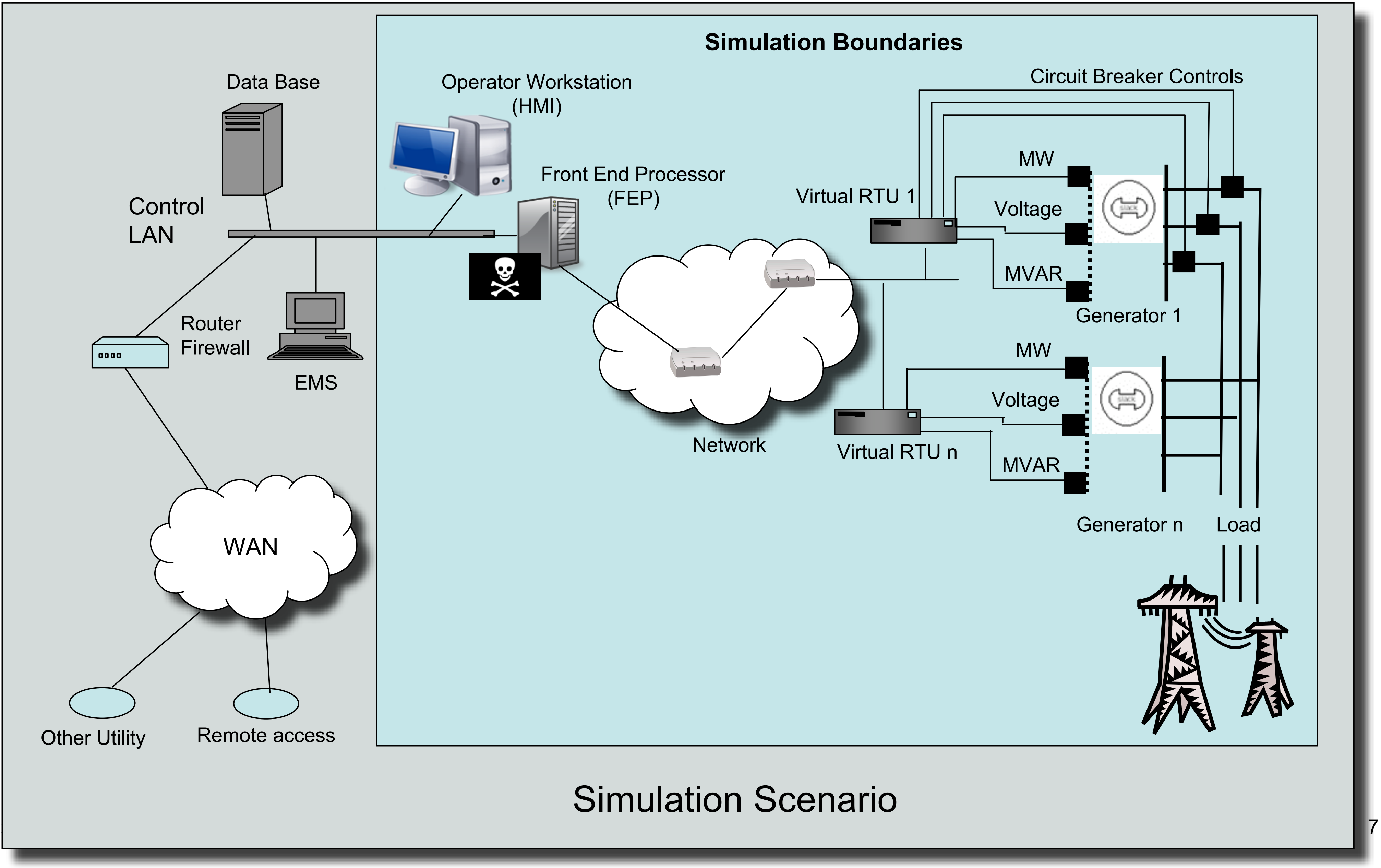
Analysis at varying levels of fidelity

- Simultaneous analysis of
  - Physical processes
  - Control Systems
  - IP & switched networked communications
- Combined analysis of
  - Power system
  - Cyber security assurance level
  - System availability
  - System performance



- Analysis of the thread from command origin to the point of the effect in the power system

Rogue Software Scenario (An Operational Analysis)



Simulation Scenario

Rogue Software Model Assumptions

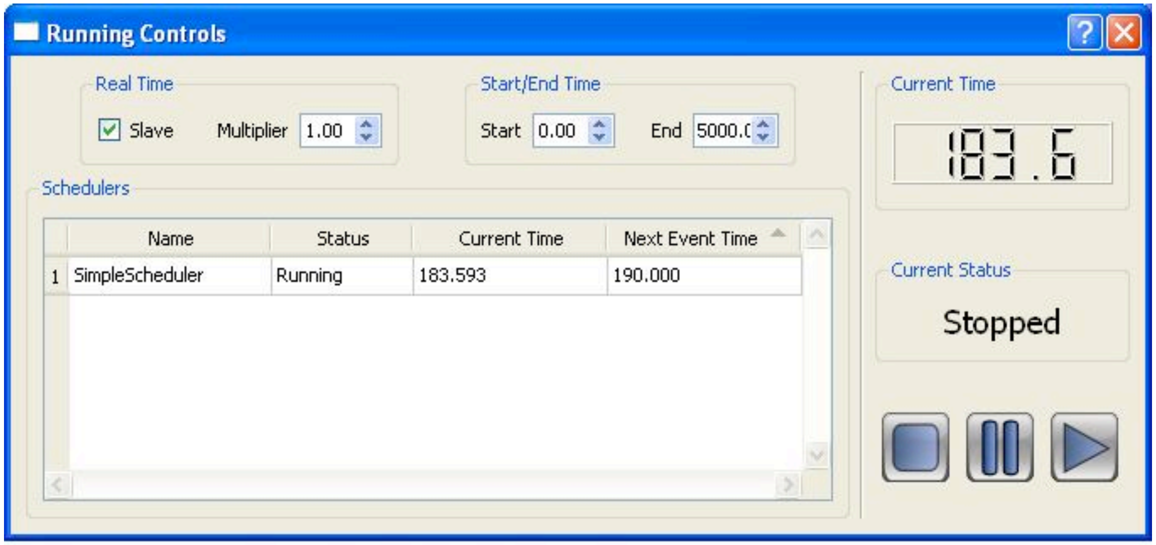
- Model focused on cyber mechanisms
  - Cyber interactions modeled using network messaging
  - Cyber threat modeled using valid network messaging attack mechanisms
- Power represented at low fidelity
  - Quasi-static power model
  - Power modeled at fidelity more appropriate for load estimation
  - Basic load shedding scheme designed to preserve power
- Model sheds load
  - Proportional to generation lost
  - Small loads shed early

Rogue Software System Simulation

VCSE Simulation Framework

Operated in both analysis and demonstration modes

- Coordinates the simulation process
- Provides network “glue” for all the components
- Provides visual insight to the simulation
- Library of simulation devices



Running Controls

Real Time

☑ Slave Multiplier 1.00

Start/End Time

Start 0.00 End 5000.0

Current Time

183.6

Schedulers

	Name	Status	Current Time	Next Event Time
1	SimpleScheduler	Running	183.593	190.000

Current Status

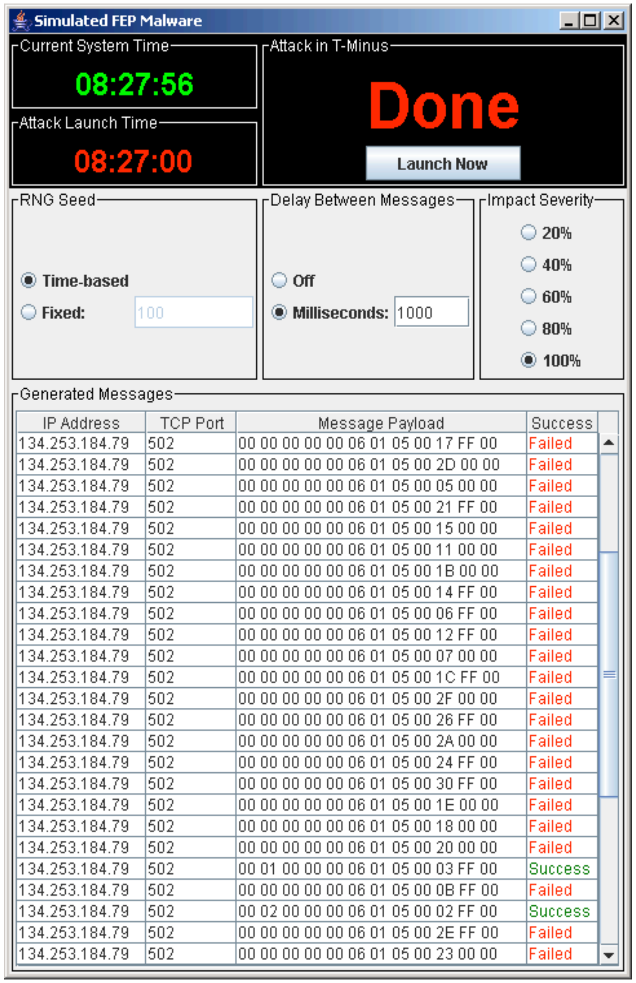
Stopped

Rogue Software Attack Simulator

Vulnerabilities & Attacks

- Real exploitations or virtual representations of how they affect the system
- Man-in-the-middle
- Rogue Software Scenario

Represents multiple malevolent Front End Processors being deployed at varying levels of effectiveness



Current System Time: 08:27:56

Attack Launch Time: 08:27:00

Attack in T-Minus: Done

RNG Seed:
● Time-based
○ Fixed: 100

Delay Between Messages:
○ Off
● Milliseconds: 1000

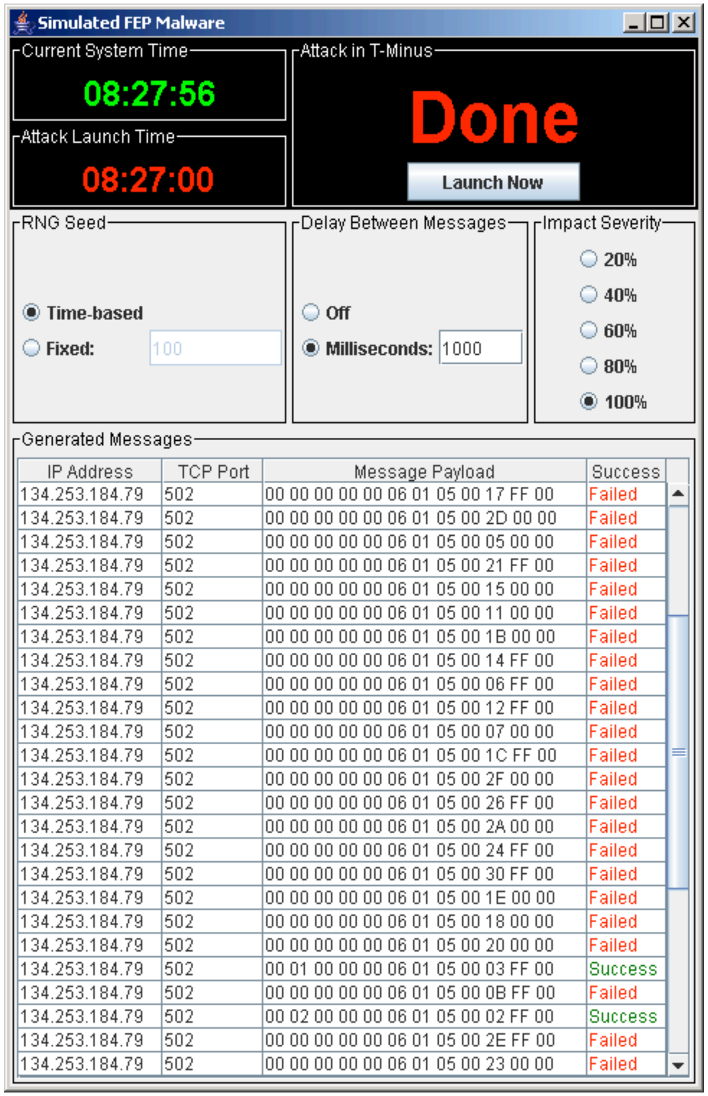
Impact Severity:
○ 20%
○ 40%
○ 60%
○ 80%
● 100%

Generated Messages

IP Address	TCP Port	Message Payload	Success
134.253.184.79	502	00 00 00 00 00 06 01 05 00 17 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 2D 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 05 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 21 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 15 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 11 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 1B 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 14 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 06 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 12 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 07 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 1C FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 2F 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 26 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 2A 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 24 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 30 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 1E 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 18 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 20 00 00	Failed
134.253.184.79	502	00 01 00 00 00 06 01 05 00 03 FF 00	Success
134.253.184.79	502	00 00 00 00 00 06 01 05 00 0B FF 00	Failed
134.253.184.79	502	00 02 00 00 00 06 01 05 00 02 FF 00	Success
134.253.184.79	502	00 00 00 00 00 06 01 05 00 2E FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 23 00 00	Failed

Rogue Software Attack Simulator

- Represents malevolent Front End Processor (FEP) functionality
- The simulation did not modify the Operator Workstation/FEP software
- Designed for Whole System Analysis
  - Message threads are analyzed from FEP to RTUs to power system devices
  - Parametric Studies: Attack severity (Impact Severity) parameters provide for an analysis of load shedding and its regional effects (which generators we tripped off and what load regions where shed)



Current System Time: 08:27:56

Attack Launch Time: 08:27:00

Attack in T-Minus: Done

RNG Seed: ● Time-based ○ Fixed: 100

Delay Between Messages: ○ Off ● Milliseconds: 1000

Impact Severity: ○ 20% ○ 40% ○ 60% ○ 80% ● 100%

Generated Messages

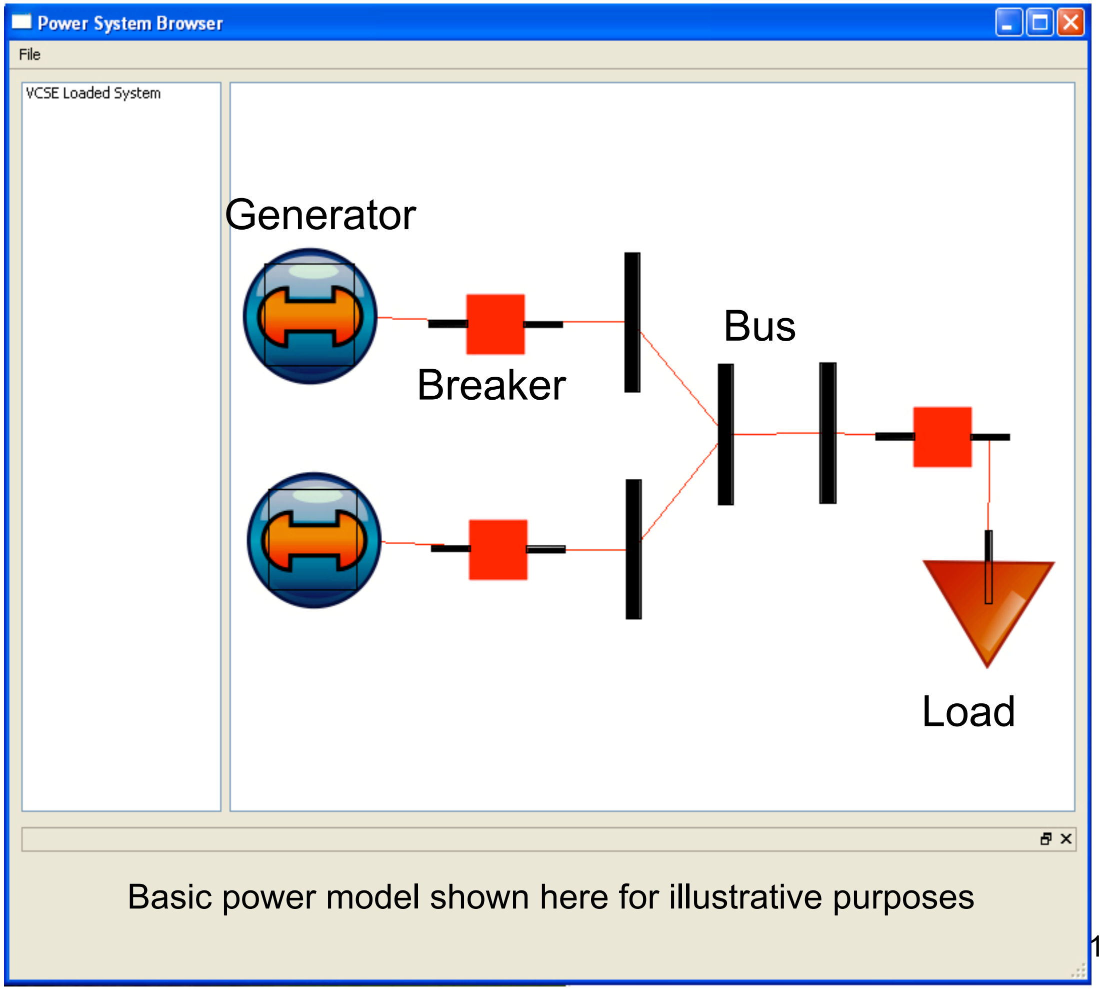
IP Address	TCP Port	Message Payload	Success
134.253.184.79	502	00 00 00 00 00 06 01 05 00 17 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 2D 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 05 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 21 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 15 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 11 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 1B 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 14 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 06 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 12 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 07 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 1C FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 2F 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 26 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 2A 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 24 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 30 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 1E 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 18 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 20 00 00	Failed
134.253.184.79	502	00 01 00 00 00 06 01 05 00 03 FF 00	Success
134.253.184.79	502	00 00 00 00 00 06 01 05 00 0B FF 00	Failed
134.253.184.79	502	00 02 00 00 00 06 01 05 00 02 FF 00	Success
134.253.184.79	502	00 00 00 00 00 06 01 05 00 2E FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 23 00 00	Failed

Rogue Software Target Simulator

Infrastructure Models

- Represents the controlled infrastructure and its response to the Control System
- Steady state power models
- Dynamic power models
- PowerWorld models (commercial)

Uses the IEEE Reliability Test System '96 Model



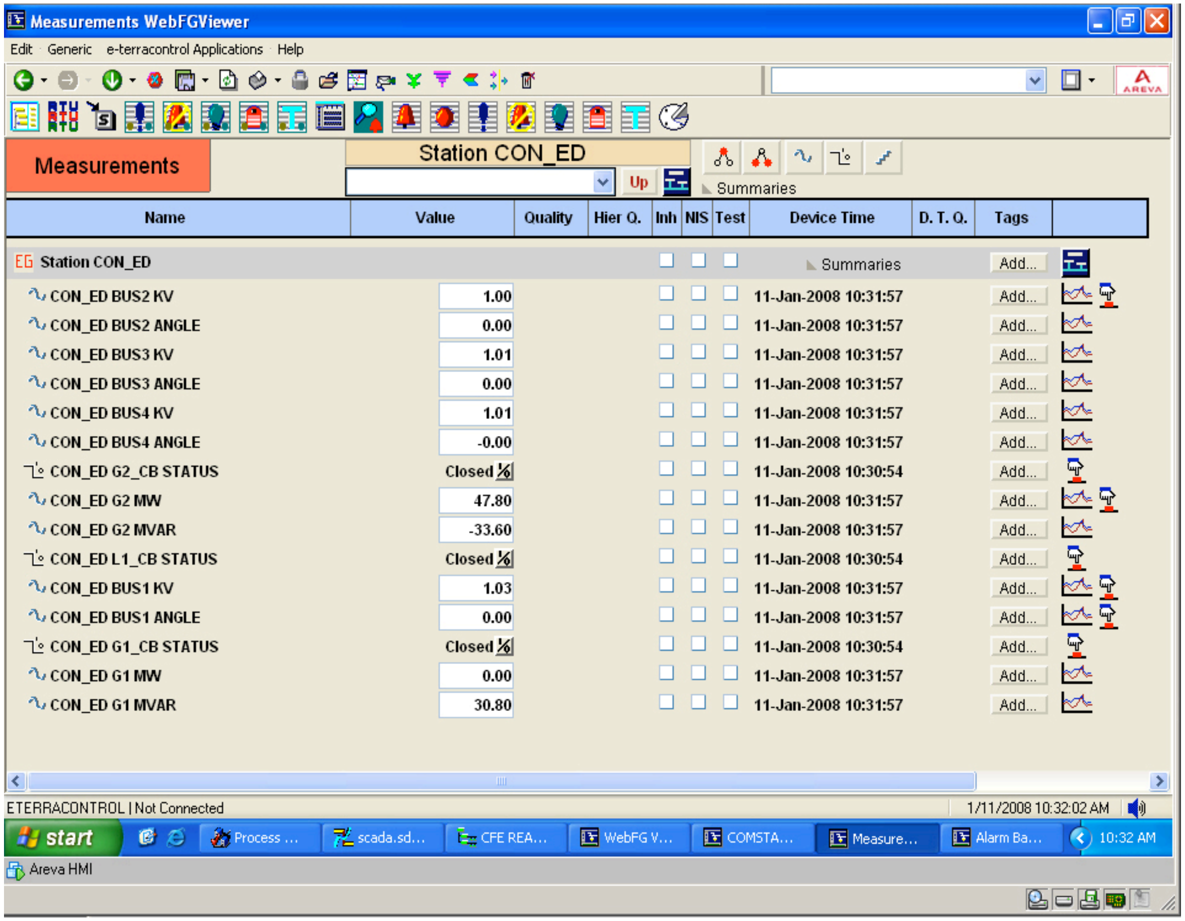
Basic power model shown here for illustrative purposes

Rogue Software Target Devices

Virtual Control Devices

24 virtual RTUs

- Simulates the control system devices and connections to the Infrastructure
- Generic Virtual Remote Terminal Units (RTU)



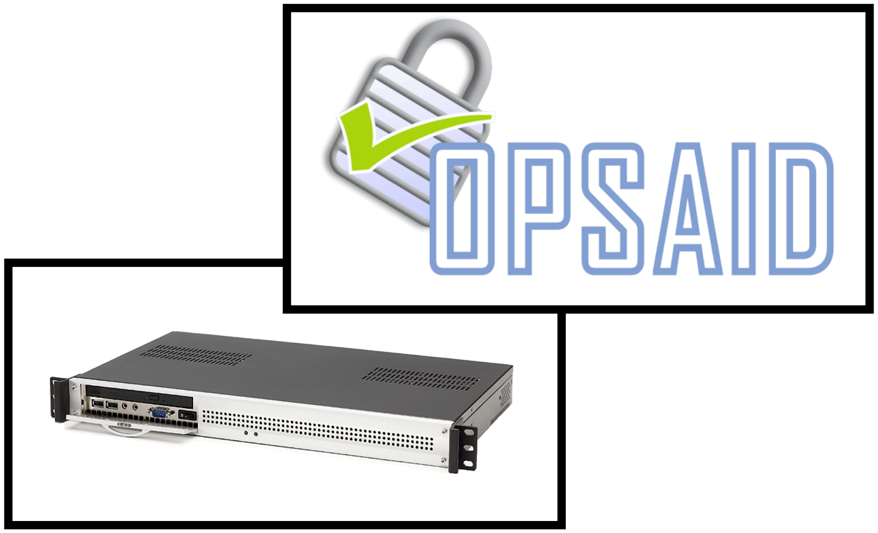
Name	Value	Quality	Hier Q.	Inh	NIS	Test	Device Time	D. T. Q.	Tags
EG Station CON_ED				□	□	□	Summaries		Add...
CON_ED BUS2 KV	1.00			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED BUS2 ANGLE	0.00			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED BUS3 KV	1.01			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED BUS3 ANGLE	0.00			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED BUS4 KV	1.01			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED BUS4 ANGLE	-0.00			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED G2_CB STATUS	Closed			□	□	□	11-Jan-2008 10:30:54		Add...
CON_ED G2 MW	47.80			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED G2 MVAR	-33.60			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED L1_CB STATUS	Closed			□	□	□	11-Jan-2008 10:30:54		Add...
CON_ED BUS1 KV	1.03			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED BUS1 ANGLE	0.00			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED G1_CB STATUS	Closed			□	□	□	11-Jan-2008 10:30:54		Add...
CON_ED G1 MW	0.00			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED G1 MVAR	30.80			□	□	□	11-Jan-2008 10:31:57		Add...

Rogue Software Mitigation Test

Cyber Security Components

Incorporates an OPSAID* compliant device which logs and alarms during the attack

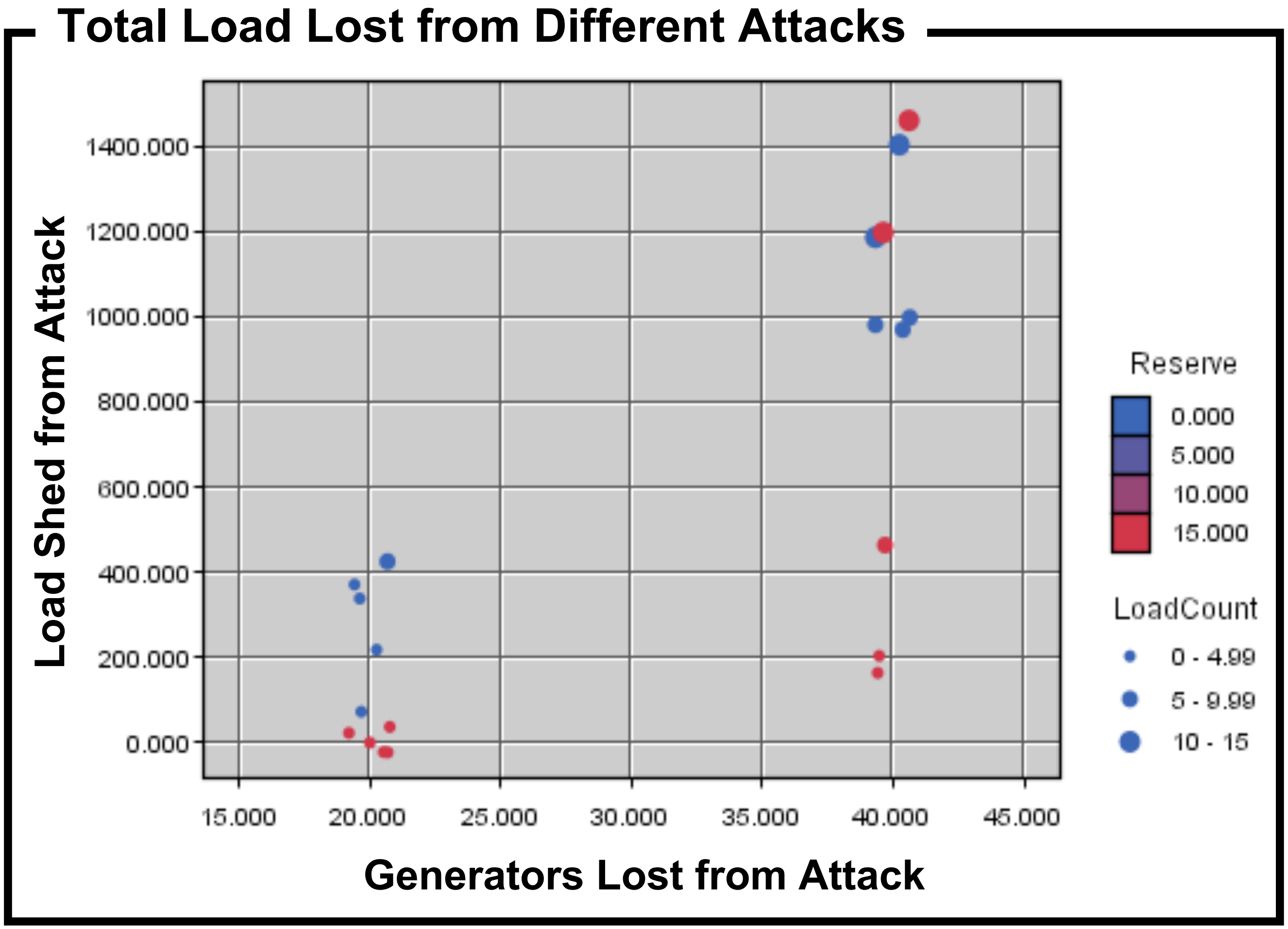
- Real or virtual components that protect or secure the cyber system
- Firewalls, router configurations, encryption devices, etc.
- OPSAID



*OPSAID: Open Process control system Security Architecture for Interoperable Design

Rogue Software Preliminary Analytic Results

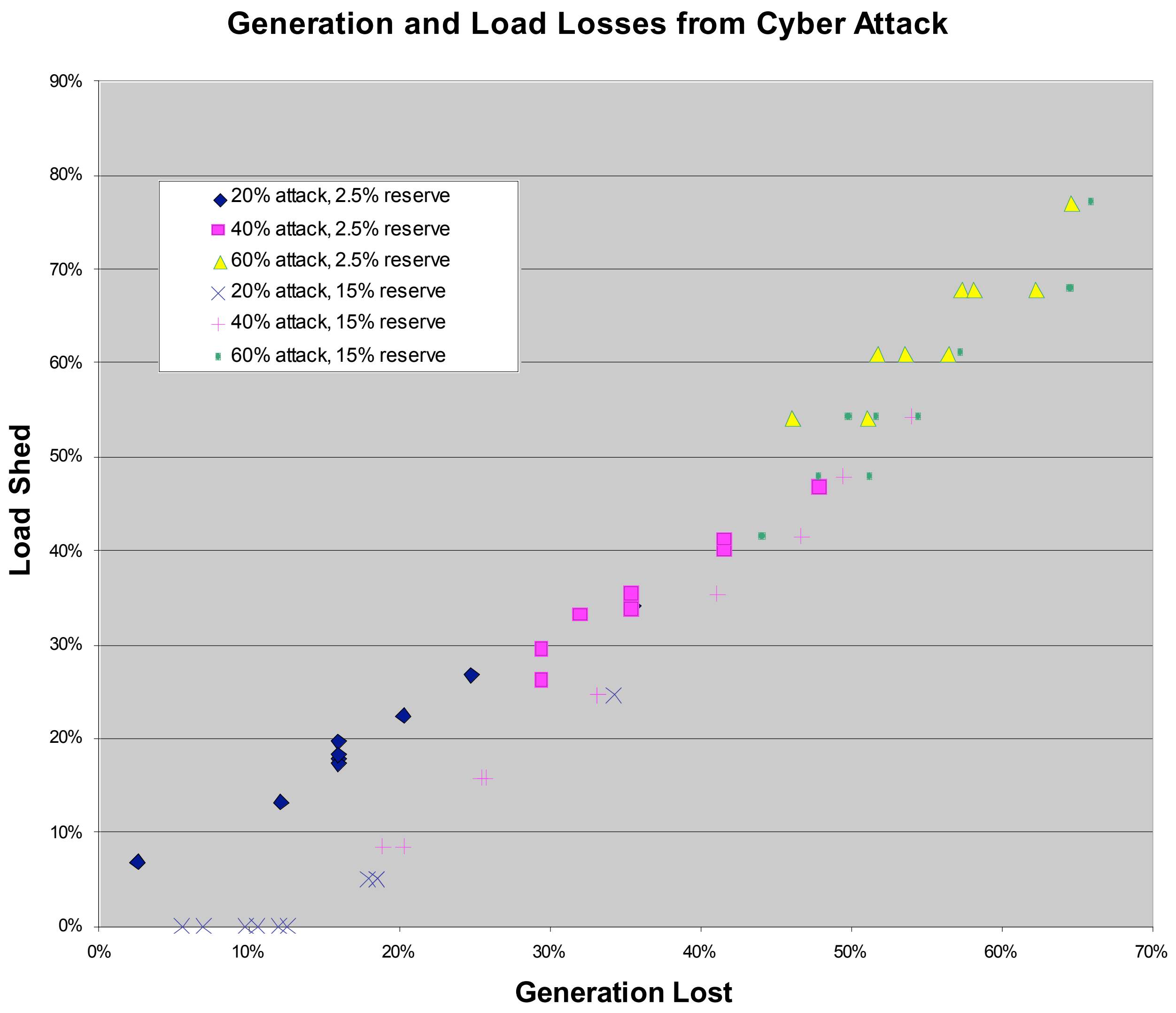
- Severity depends upon which generators get hit and how many get hit
- Significant impact created when 40% of generators hit



Total Load Lost from Different Attacks

Study Parameters
- 17 Regions
- 2,850 MW Total Load (demand)
- 15 and 2.5% Spinning Reserve

Rogue Software Preliminary Analytic Results



- Impact spans scale of operation
  - Load Shed within 10% of (Attack – Reserve) %
- Large spinning reserve helped mitigate smaller attacks

Observations from Study

- Not a surprise that large-scale attack takes down system
- Proportional load shed to generation lost is likely an artifact of this low-fidelity model
- Further Studies Suggested
  - Improve Power Fidelity
    - Dynamic Simulation
    - Sophisticated Load Shedding Mechanisms
  - Investigate whether key features impact total load shed:
    - Speed of attack
    - Protection system design
    - Direction of attack (explain)

Analysis Conclusions

- The scenario shows that such an event:
  - Is feasible
  - Can produce significant effects based on
    - Ubiquity of the malware distribution
    - The capabilities (software engineering & access to the development cycle) and motives of the malicious agents
- This malicious software is difficult to detect
  - Through exhausted software code inspection
  - During operation through previously established network monitoring rules

🟥 Red:	High Defender Effect
🟧 Orange:	Moderate Defender Effect
🟩 Green:	Low Defender Effect

Cyber Effects	**H**
Attack Feasibility	**H**
Potential worst case Effectiveness (based on ubiquity)	**H**
Expected Feasibility with Software Inspection	**M**
Expected Feasibility with Network Monitoring	**M**

The Rogue Software attack is fictitious and not based on intelligence or known adversary capabilities

NSTB

National SCADA Test Bed

enhancing control systems security in the energy sector

VCSE Demonstration

U.S. Department of Energy
Office of Electricity Delivery
and Energy Reliability

Sandia National Laboratories

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.